基于虚拟移动的 IPv6 主动防御方案 *

孔亚洲，张连成，王振兴

(数学工程与先进计算国家重点实验室，郑州 450002)

摘 要： 现有通过地址跳变对 IPv6 节点进行防护的技术依赖时间同步或事件同步，利用 IPv6 的良好移动特性和多转交地址注册机制，提出一种基于虚拟移动的 IPv6 主动防御方案。通过为 IPv6 节点分配动态变化的转交地址，使其呈现出在网络内不断移动的特征，降低攻击者对其实施攻击概率的同时，能够保证通信的持续。理论分析和实验测试表明，方案具有良好的抗攻击能力且较小的系统开销。

关键词： IPv6；虚拟移动；主动防御；方案

中图分类号： TP393.08 doi: 10.3969/j.issn.1001-3695.2018.01.0045

Proactive defense scheme of IPv6 based on virtual mobile

Kong Yazhou, Zhang Liancheng, Wang Zhenxing

(*State Key Laboratory of Mathematical Engineering & Advanced Computing*, *Zhengzhou* 450002, *China*)

Abstract: The existing technologies for protecting IPv6 nodes by address hopping rely on time synchronization or event synchronization, utilizing the good mobility feature of IPv6 and multiple care-of address registration mechanisms, this paper proposed a proactive defense scheme of IPv6 based on virtual mobile. By assigning a dynamically changing care-of address to an IPv6 node, the IPv6 node presented the continuously moving feature in the network, reduced the attack probability of an attacker, and ensured the continuity of communications. Theoretical analysis and experimental tests show that the scheme has good anti-attack ability and less system overhead.

Key words: IPv6; virtual mobile; proactive defense; scheme

0 引言

2016 年 11 月 7 日，互联网架构委员会（Internet Architecture Board，IAB）发表声明称，建议互联网工程任务组（Internet Engineering Task Force，IETF）等标准开发组织及合作伙伴放弃在新协议标准中兼容 IPv4，用行动支持并实施 IPv6 在全球范围内的部署[1]。2017 年 11 月 26 日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》[2]（简称“计划”），“计划”要求不仅要实现移动互联网全面支持 IPv6，还要强化网络安全保障。

随着 IPv6 部署的广泛深入，越来越多的网络服务正逐步迁移到 IPv6 网络，包括 Web 服务器、邮件服务器、域名服务器等。由于 IPv6 拥有 128 位地址空间，使得每个节点均能分配一个全球可路由单播地址，且可保持永久不变。因此，在 IPv6 网络环境中，提供网络服务的重要节点更易遭受来自攻击者的攻击[3]，其中最常见且难以防护的攻击包括拒绝服务（denial of service，DoS）攻击、分布式拒绝服务（distributed denial of service，DDoS）攻击等。

针对网络的确定性和静态性带来的网络易攻难守等挑战，美国提出一种“改变游戏规则”的积极主动的网络防御思想，即移动目标防御（moving target defense，MTD）[4]，通过动态、持续的变化以显著增加攻击者的攻击难度，降低其攻击成功率。利用这一防御思想，研究人员已经在网络层设计并开发出了多种具体的防御机制。动态网络地址转换（dynamic network address translation，DyNAT）[5]是一种在数据包被路由转发之前，动态变化其地址与端口信息来抵抗嗅探攻击的技术，该技术依赖集中网关的安全性，存在通信失败的可能；网络地址随机化（network address space randomization，NASR）[6]是一种通过修改网络内动态主机配置协议（dynamic host configuration protocol，DHCP）服务器来动态更改 IP 地址变化频率来抵抗蠕虫攻击的技术，该技术部署成本较高，且只能实现局域网（local area network，LAN）内的地址随机化；端口跳变（port hopping）是一种通过动态变化 TCP/UDP 端口号来抵抗 DoS/DDoS 攻击的技术；Lee 等人[7]提出一种通过在服务器和用户之间共享私钥进行 TCP/UDP 端口跳变的技术，该技术能够有效阻止攻击者对服务器进行攻击，但是其依赖严格时间同步，无法适用于网络延时较大的网络中；Badishi 等人[8]提出一种基于端口的配给信道机制，利用伪随机函数使不同信道在不同时刻使用不同的

收稿日期： 2018-01-16；**修回日期：** 2018-03-09 **基金项目：** 国家自然科学基金重点资助项目（61402526）

作者简介： 孔亚洲（1989-），男，河南濮阳人，博士研究生，主要研究方向为 IPv6 网络安全（coyote0916@163.com）；张连成（1982-），男，河南商丘人，讲师，博士，主要研究方向为 SDN 网络安全；王振兴（1959-），男，河北晋州人，教授，博士，主要研究方向为 IPv6 网络安全.

端口通信，这一机制的安全性依赖于 ACK 报文，若 ACK 报文被截获，攻击者即可对目标节点实施攻击；石乐义等人[9]提出服务跳变（service hopping）和端跳变（end hopping）的概念，通过伪随机跳变图来动态地变化通信双方或一方的 IP 地址、端口、时隙、加密算法、通信协议等信息，以增加攻击难度与成本；Jafarian 等人[10]提出一种 OF-RHM（OpenFlow random host mutation）技术，利用 OpenFlow 快速变换主机虚拟 IP，OpenFlow 实现虚拟 IP 与真实 IP 的转换，从而增加攻击难度。由于 OF-RHM 部署困难，Al-Shaer 等人[11]提出一种 RHM（random host mutation）技术，利用低频变换和高频变换来给主机分配虚拟 IP。为提高变化机制安全性，Jafarian 等人[12]提出一种 STAM（spatio-temporal address mutation）机制来实现动态变化主机与 IP 地址的绑定关系，每个主机对应一个瞬时 IP，且每个瞬时 IP 只能在指定时间间隔内与另一特定主机通信。MT6D（moving target IPv6 defense）[13]是一种在 IPv6 网络环境下 MTD 的具体实现方法，通信双方以 EUI-64 接口标志符（interface identifier，IID）、共享密钥及系统时间为参数，经过哈希计算后生成新的 IID，增加了攻击成本与复杂度；刘慧生等人[14]提出一种利用 IPv6 多穴特性使主机地址在多个地址域内动态变化的技术 MHH-PD6，增加了攻击者流量监听及 DoS 攻击的难度。

综上所述，现有的可有效阻止或降低 IPv6 节点遭受 DoS 攻击的技术（以 MT6D 和 MHH-PD6 为例）主要存在以下不足之处：a)MT6D 在通信地址动态改变的过程中存在地址冲突的可能，从而造成丢包或会话中断现象；b)MT6D 依赖严格时间同步，无法适应网络延迟较大或网络拥塞的网络环境；c)MHH-PD6 依赖跳变服务器的安全性，跳变服务器存在被 DoS 攻击的可能；d)MHH-PD6 需要所在网络接入多条链路，适用范围受限。

针对现有研究技术的不足之处，本文提出一种基于虚拟移动的 IPv6 抗 DoS 攻击方案，利用 IPv6 的良好移动特性支持，提出虚拟移动思想，即为受保护 IPv6 节点分配动态变化的转交地址（care-of address，CoA），使攻击者无法准确辨识目标节点是否发生真实移动及其位置，从而无法对其实施 DoS 攻击。此外，由于移动 IPv6（mobile IPv6，MIPv6）允许 IPv6 节点能够在移动（即改变其 CoA）的同时保持当前连接，因此该方案不依赖时钟同步或事件同步机制，能够适应较复杂的网络环境且保持通信的持续不断。

1　ADVM 方案

本文提出的虚拟移动（virtual mobile，VM）包含两方面含义：一是 IPv6 节点未发生真实移动，而是利用 IPv6 对移动的良好支持，使其对外呈现出移动的表征；二是 IPv6 节点发生真实移动，使其对外呈现出移动位置动态变化的特点，无法辨识其移动的真伪。接下来，本章将对 ADVM 方案的基本结构、工作流程进行详细描述。

1.1　ADVM 结构组成

定义 1　IPv6 虚拟移动节点（virtual mobile node for IPv6，VMN）。受 ADVM 方案保护的 IPv6 节点。

定义 2　转交地址集（set of care-of addresses）。VMN 用于呈现虚拟移动特征的地址集合，$C=\{coa_1,coa_2,\ldots,coa_n\},n\in\mathbb{Z}$。

定义 3　IPv6 虚拟移动代理（virtual mobile agent for IPv6，VMA）。与 VMN 处于不同子网的 IPv6 节点，$A=\{vma_1,vma_2,\ldots,vma_n\},n\in\mathbb{Z}$，为 VMN 转发通信数据包。

定义 4　通信对端（corresponding node，CN）。与 VMN 进行通信的对端节点，$N=\{cn_1,cn_2,\ldots,cn_l\},l\in\mathbb{Z}$。

ADVM 的基本结构如图 1 所示。

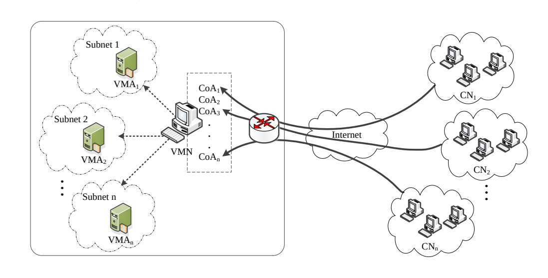


图 1　ADVM 基本结构

ADVM 方案基本思想是：在于 CN 进行通信过程中，VMN 从集合 A 中随机选取一个子集 $A_{subset}=\{vma_i,vma_{i+1},\ldots,vma_j\},i,j\geq 1,且i,j\in\mathbb{Z}$，其对应的转交地址子集为 $C_{subset}=\{coa_i,coa_{i+1},\ldots,coa_j\},i,j\geq 1,且i,j\in\mathbb{Z}$，VMN 将通信对端分为若干个组 $G=\left\{\left(\overbrace{cn_k,cn_{k+1},\ldots,cn_m}^{m-k+1}\right)\ldots\left(\overbrace{cn_u,cn_{u+1},\ldots,cn_v}^{v-u+1}\right)\right\},cn\in N$，每个组中的成员与数量均是随机的，VMN 将转交地址子集按照 RFC 5648[15]中定义的多转交地址注册（multiple care-of addresses registration）过程随机通知给通信对端组，从而达到有效保护 VMN 免受 DoS 攻击的目的。

1.2　ADVM 基本流程

ADVM 方案的基本流程如图 2 所示。其中 Alice 为 IPv6 虚拟移动节点 VMN，$Bob=\{Bob_i\,|\,1\leq i\leq n\},n\in\mathbb{Z}$ 为通信对端集合，$A=\{A_j,1\leq j\leq m\},m\in\mathbb{Z}$ 为 IPv6 虚拟移动代理集合 VMA。接下来对其工作过程进行详细阐述。

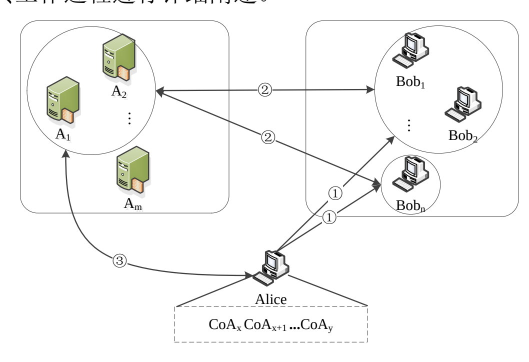


图 2　ADVM 基本流程

1)Alice 向 VMA 发起虚拟移动注册

首先，虚拟移动节点 Alice 从 VMA 的集合 A 及其转交地址集合 C 中随机选取一个非空子集构成集合 $S=\{\langle A_i,CoA_i\rangle\,|\,A_i\in A,CoA_i\in C,1\leq i\leq n\},n\in\mathbb{Z}$，并向集合中的每个 VMA 发送身份注册报文 Reg_{VMN}，虚拟移动代理验证 Alice 的身份后，

向其回复身份确认报文 Ack_{VMA}。至此，集合 S 中的每个 VMA 将作为 Alice 的通信中转节点，负责 Alice 与通信对端之间通信数据的转发，该注册过程经过随机变化的时间间隔 τ 就会执行一次，使 Alice 呈现出在 IPv6 子网间不断移动的假象，增加攻击成本及复杂度。该过程可表示为：

a）Alice： $select(S)$ 。

b） $Alice \to S: Reg_{VMN}(HoA_{Alice}, ID_{Alice})$ 。

c） $S \to Alice: Ack_{VMA}(CoA_S, ID_S)$ 。

2)多转交地址注册

在该过程中，Alice 先从通信对端的集合 Bob 中选取 z 个非空真子集 $Q_1, Q_2, ..., Q_z$ ，且 $Bob = Q_1 \cup Q_2 \cup ... \cup Q_z$ ， $\forall i \neq j, Q_i \cap Q_j = \varnothing$；然后 Alice 从集合 S 的非空子集中选取 z 个子集，并将这些集合中的转交地址以绑定更新（binding update，BU）报文的方式通知所有通信对端，这些 BU 报文增加了绑定标志符选项（binding identification number，BID）；之后每个集合中的通信对端回复绑定确认（binding acknowlegement，BA）消息。该过程可表示为：

a）Alice： $select(Q_1, Q_2, ..., Q_z)$ 。

b） $Alice \to Q_i: BU(BID_i, HoA_{Alice}, CoA_S)$ 。

c） $Q_i \to Alice: BA(HoA_{Alice}, CoA_S)$ 。

3) 返回可路由过程

RFC 6275 中描述了路由优化过程，即移动节点和通信对端之间可以直接发送通信数据。返回可路由过程（return routability procedure，RRP）是为验证移动节点既可以通过它的本地地址到达，也可以通过它的转交地址到达，从而防止绑定更新欺骗和 DoS 攻击。在 ADVM 方案中，RRP 过程如图 3 所示。

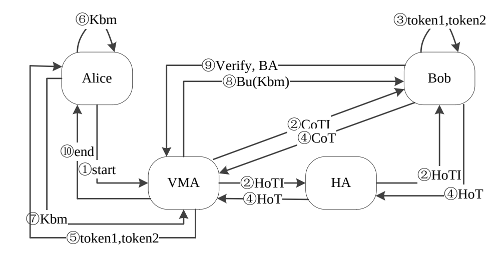


图 3　ADVM 中 RRP 的处理

a）Alice 向 VMA 发送 RRP 启动信号，随后 VMA 向 Bob 发送 HoTI（home test init）和 CoTI（care-of test Init）消息。其中，HoTI 先经过隧道发送给 HA，然后由 HA 发送给 Bob，CoTI 则由 VMA 直接发送给 Bob。该过程可表示为：

(a) $Alice \to S: start$

(b) $S \to HA \to Bob: HoTI$ ， $S \to Bob: CoTI$

b）Bob 收到 HoTI 和 CoTI 消息后，生成本地地址令牌 $token1$，转交地址令牌 $token2$，然后 Bob 将 $token1$ 置于 HoT 消息中经由 HA 发送给 VMA，将 $token2$ 置于 CoT 消息中直接发送给 VMA。该过程可表示为：

(c) $Bob: generate(token1, token2)$

(d) $Bob \to HA \to S: HoT(token1)$

， $Bob \to S: CoT(token2)$

c）VMA 收到后将 $token1$ 和 $token2$ 发给 Alice，随后 Alice 生成一个 Kbm 并发给 VMA，VMA 向 Bob 发送由 Kbm 加密的绑定更新消息，Bob 收到该消息后对 Kbm 进行认证。如果认证通过，则根据 BU 消息更新绑定缓存并回复绑定确认消息；否则，不做任何操作。该过程可表示为：

(e) $S \to Alice: packet(token1, token2, ID_S)$ 。

(f) $Alice: generate(Kbm, token1, token2)$ 。

(g) $Alice \to S: packet(Kbm, ID_{Alice})$ 。

(h) $S \to Bob: BU_{Kbm}$ 。

(i) $Bob: Verify(Kbm), if\ true,$

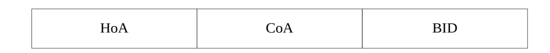
$update$ and $BA, else, do\ nothing$ 。

(j) $S \to Alice: end$ 。

经过上述过程，即使所在网络环境需要执行返回可路由过程，ADVM 依然可以实现对 VMN 的有效防护。

4)通信传输过程

通信对端的绑定缓存（Binding Cache）结构如图 4 所示，



HoA	CoA	BID

图 4　绑定缓存结构

当 Bob 与 Alice 进行通信时，首先，按照 BID 的值从绑定缓存中随机一条表项，与表项对应的 CoA 进行通信。在通信过程中采用“先选取，后删除”策略，即通信时 Bob 先选取下一刻将使用的 CoA，当通信切换到新的 CoA 之后，再将之前的缓存表项删除。VMA 收到消息后，对数据包进行排序操作后，将这些数据包转发给 Alice。然后，Alice 根据数据包中的标记进行重组，至此，Alice 的数据接收过程结束。之后，Alice 将回复数据包按此逆过程进行传输，直至 Bob 完成接收过程，至此，整个通信传输过程结束。

1.3　虚拟位置漂移算法

虚拟位置漂移算法（virtual location drift algorithm，VLDA）是对虚拟移动代理进行随机选取、对通信对端进行随机分组的过程，遇到以下三种情况将会执行该算法：a）每隔时间间隔 τ 就会执行一次；b）虚拟移动代理有更新或删除变化；c）通信对端的集合有变化。

算法 1　VLDA 算法

Algorithm VLDA

输入： VMA，CN.

输出： S，Bob.

Start

S=Select(VMA)；//从 VMA 中选取一个非空子集

CN_R=Calcu(CN)；//将 CN 分成若干个非空真子集

//从 CN_R 中随机选取若干个真子集且满足以下条件

$CN = Bob_i \cup Bob_j$ ， 当 $i \neq j$ 时, $Bob_i \cap Bob_j = \varnothing$

Bob=SelectFrom(CN_R)；

End

该算法为 ADVM 方案提供了两方面的安全性，一是虚拟移动代理集合的随机性，使攻击者对虚拟移动节点的追踪更加困难，提高了攻击难度；二是通信对端的分组随机性，使攻击者对通信流量的分析更加复杂，提高了攻击成本。

2　ADVM 方案分析

2.1　ADVM 安全性分析

本节主要从以下两个方面对 ADVM 的安全性进行分析：a）攻击者扫描速率与 ADVM 安全性之间的关系；b）攻击者数量与 ADVM 安全性之间的关系。

1）攻击者扫描速率与 ADVM 安全性之间的关系

假设防御者在 t 时刻选用的 VMA 的数量一共有 η 个， $\chi(t)$ 是攻击者在 t 时刻无法确定的 VMA 的数量，假设攻击者对 VMA 的扫描是独立泊松过程，攻击者所用扫描时间为 T_{scan} ，那

么攻击者对每个 VMA 的平均扫描速率为 $1/\eta T_{scan}$，每个 VMA 的变化时间间隔是独立的，且服从指数分布（平均 $T_{success}=1/\xi$），假设防御者选取 VMA 的时间是随机变化的，那么 χ 可建模为一个连续时间的齐次马尔科夫链，其转移到状态 s 的转移速率矩阵可表示为

$$\mathbf{Q}=\begin{bmatrix}-q_{00} & q_{01} & \cdots & q_{0\eta}\\ q_{10} & -q_{11} & \cdots & q_{1\eta}\\ \vdots & \vdots & & \vdots\\ q_{\eta 0} & q_{\eta 1} & \cdots & -q_{\eta\eta}\end{bmatrix},\text{其中,}$$

$$q_{s,s-1}=\zeta\ ,1\le s\le\eta\ \ q_{s,\eta}=\xi,0\le s\le\eta-1$$

攻击者的平均扫描速率 $\zeta=1/T_{scan}$，代表攻击者锁定 VMA 的速度。

χ 的稳态分布 π 满足平衡方程 $\pi'\mathbf{Q}=0'$，其中转移速率矩阵 $\mathbf{Q}=[q_{i,j}]$，且 $q_{i,j}=-\sum_{j\neq i}q_{i,j}$。令 $\varphi=\frac{\zeta}{\xi}=\frac{T_{success}}{T_{scan}}$，且 $\gamma=\frac{\zeta}{\zeta+\xi}=\frac{\varphi}{\varphi+1}$，求解平衡方程得

$$\pi_i=\begin{cases}\gamma^{\eta}, & ,i=0\\ \gamma^{\eta-i+1}(1/\gamma-1) & ,0<i\le\eta\end{cases}$$，因此，

χ 的期望记为

$$\begin{aligned}E\chi&=\sum_{i=0}^{\eta}i\pi_i\\&=\eta-\frac{\gamma\left(1-\gamma^{\eta}\right)}{1-\gamma}\\&=\eta-\varphi\left(1-\left(\frac{\varphi}{\varphi+1}\right)^{\eta}\right)\end{aligned}$$

由上可得:

结论 1　$E\chi$ 与 φ 成反比，即使攻击者采用较高的扫描速率，也只能获取较少的 VMA 的信息，增加了攻击者的攻击难度和复杂度。

2）攻击者数量与 ADVM 安全性之间的关系

首先，给出涉及到的符号及其说明，如表 1 所示。

表 1　符号说明

符号	含义
N	所有通信对端的数目
N_a	所有假冒通信对端的攻击者数目
N_b	所有合法通信对端数目
τ	跳变时间间隔
N_{CoA}	跳变间隔内 VMA 数目
N_{c_k}	使用注册地址 CoA_k 的通信对端数目
p_{CoA_k}	注册地址 CoA_k 不被扫描发现的概率
N_{ba}	与攻击者处于同组的通信对端数目
$N_{ba'}$	与攻击者不处于同组的通信对端数目
p_e	通信对端通信成功的概率

由表可知，$N=N_a+N_b$，与攻击者不处于同组的通信对端的数目为

$$N_{ba'}=\sum_{k=1}^{N_{CoA}}p_{CoA_k}N_{c_k}$$

假设通信对端的数目按照 CoA 的数目均匀分布，那么 $N_{c_k}=\frac{N}{N_{CoA}},k\ge1$，使用注册地址 CoA_k 的通信对端不被锁定的概率为

$$p_{CoA_k}=\frac{\binom{N-N_a}{N_{c_k}}}{\binom{N}{N_{c_k}}}$$

其中：$\binom{N-N_a}{N_{c_k}}$ 是 $N-N_a$ 中大小为 N_{c_k} 的真子集的个数；$\binom{N}{N_{c_k}}$ 是 N 的大小为 N_{c_k} 的真子集的个数。因此，

$$E\left(N_{ba'}\right)=\sum_{k=1}^{N_{CoA}}\frac{\binom{N-N_a}{N_{c_k}}}{\binom{N}{N_{c_k}}}N_{c_k}$$

假设通信对端均匀分布于各个真子集，因此，

$$E\left(N_{ba'}\right)=\frac{\binom{N-N_a}{N_{c_k}}}{\binom{N}{N_{c_k}}}\times N$$

根据斯特林公式，$n!\approx\left(\frac{n}{e}\right)^n\sqrt{2\pi n}$，假设 $N_a\ll N$，那么：

$$E\left(N_{ba'}\right)=N\times\left(\frac{N-N_a}{N}\right)^{N_{c_k}}=N\times\left(1-\frac{N_a}{N}\right)^{N/CoA_k}$$

那么，通信对端通过 VMA 成功进行数据传输的概率为

$$p_e=\frac{N}{N_b}\left(1-\frac{N_a}{N}\right)^{N/CoA_k}$$

由上可得：

结论 2　攻击者数量的增加并不能显著降低通信对端的通信效率，增加了攻击复杂度，提升了网络安全性。

2.2　ADVM 性能分析

由 1.2 节可知，与正常 IPv6 通信相比，VMA 的选取和数据转发有可能带来一定的时延。接下来，本节将对 ADVM 对通信性能的影响进行分析。

1）正常情况下，IPv6 通信时延

首先，对正常情况下 IPv6 节点间的通信时延进行分析。当通信发起者为固定节点时，通信时延主要是路径传输时延，记为 T_{path}，当通信发起者为移动节点时，通信时延主要包括移动节点完成链路切换的时延 $T_{handover}$，当移动节点移动到新的外地链路时，要执行地址自动配置，此阶段所耗时间记为 T_{config}；之后，移动节点要与通信对端完成路由优化过程，所用时间记为 $T_{optimal}$；最后，通信对端与移动节点进行通信时的路径传输时延为 T_{path}。因此，正常情况下，IPv6 通信时延可记为

$$T_{normal}=\begin{cases}T_{path}, & (\text{发起者为固定节点})\\ T_{path}+T_{handover}+T_{config}+T_{optimal} & (\text{发起者为移动节点})\end{cases}$$

2）ADVM 通信时延

在 ADVM 方案中，若 VMN 是固定节点，那么 ADVM 的通信时延主要包括 VMN 每隔时间 τ 执行一次算法的时间，记为 T_{alg}。ADVM 向选取的 VMA 发起注册的时间 T_{reg}，VMA 返回确认信息的时间 T_{ack}。VMN 向通信对端发起多转交地址注册的过程中，所需时间包括绑定更新时间和绑定确认时间，分别记为 T_{BU} 和 T_{BA}。路径传输时延包括通信对端到 VMA 的时间和 VMA 到 VMN 的时间，分别记为 $T_{CN\to VMA}$ 和 $T_{VMA\to VMN}$。若 VMN 是移动节点，除去上述过程的时延外，还包括 VMN 完成链路切换的时延 $T_{handover}$ 和 VMN 移动到外地链路后，完成地址自动配置所花费的时延 T_{config}。因此，ADVM 方案的通信时延可记为

$$T_{ADVM}=\begin{cases}T_{alg}+T_{reg}+T_{ack}+T_{BU}+\\ T_{BA}+T_{CN\to VMA}+T_{VMA\to VMN}\\ \qquad(\text{当VMN为固定节点})\\ T_{alg}+T_{reg}+T_{ack}+T_{BU}+\\ T_{BA}+T_{CN\to VMA}+T_{VMA\to VMN}+T_{handover}+T_{config}\\ \qquad(\text{当VMN为移动节点})\end{cases}$$

其中，由于 ADVM 中涉及的绑定更新与确认，数据传输过程与正常情况下的时延并无区别，因此，

$T_{optimal}=T_{BU}+T_{BA}$，

$T_{path}=T_{CN\to VMA}=T_{VMA\to VMN}$

因此，ADVM 的通信时延可简化为

$$T_{ADVM}=\begin{cases}T_{alg}+T_{reg}+T_{ack}\\ +T_{optimal}+2T_{path}\\ \qquad(\text{当VMN为固定节点})\\ T_{alg}+T_{reg}+T_{ack}\\ +T_{optimal}+2T_{path}+T_{handover}+T_{config}\\ \qquad(\text{当VMN为移动节点})\end{cases}$$

因此，与正常通信相比，ADVM 方案的额外开销可记为

$$T_{extra}=\begin{cases}T_{alg}+T_{reg}+T_{ack}+T_{optimal}+T_{path}\\ \qquad(\text{当VMN为固定节点})\\ T_{alg}+T_{reg}+T_{ack}+T_{path}\\ \qquad(\text{当VMN为移动节点})\end{cases}$$

由此可知，当 VMN 为固定节点时，即 VMN 并未发生真实移动时，为虚拟其移动的情景，额外开销主要是执行算法的开销，进行虚拟注册的时间开销及数据传输开销；当 VMN 为移动节点时，即 VMN 发生真实移动，但虚拟其移动至其他子网的情景，额外开销主要是执行算法的开销，进行虚拟注册的时间开销及数据传输开销，但无需进行一次路由优化的时间开销。

3　实验测试与分析

利用移动 IPv6 的开源实现 UMIP，在 Ubuntu 17.04 操作系统上实现了 ADVM 方案，通过接入 CERNET2 搭建了如图 5 所示的验证环境。

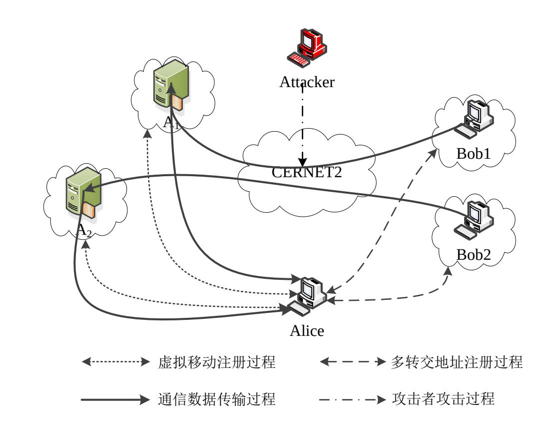


图 5　实验测试拓扑

其中，A1 和 A2 为虚拟移动代理，Bob1 和 Bob2 为通信对端，Alice 为虚拟移动节点，Attacker 为攻击者。参数配置如表 2 所示。

表 2　参数配置

节点	IPv6 地址	操作系统
A1	2001:da8:2017::ad12	Ubuntu 17.04
A2	2001:da8:2018::cd49	Ubuntu 17.04
Bob1	2001:da8:2019::38e1	Windows 8
Bob2	2001:da8:2020::af09	Ubuntu 17.04
Alice	2001:da8:2021::ac22	Ubuntu 17.04
Attacker	2001:da8:2022::ff03	Windows 8

3.1　ADVM 开销测试

为测试 ADVM 方案的开销，主要从以下两种场景对其开销进行测试：a）Alice 为固定节点；b）Alice 为移动节点。

针对第一种场景，依据虚拟位置漂移算法，Alice 选取 A1 和 A2 的 IPv6 地址为 CoA，并分别向 Bob1 和 Bob2 进行多转交地址注册，通过在 Alice 与 Bob1 和 Bob2 之间传输不同大小的文件来测试 ADVM 的开销，其测试结果如图 6 所示。

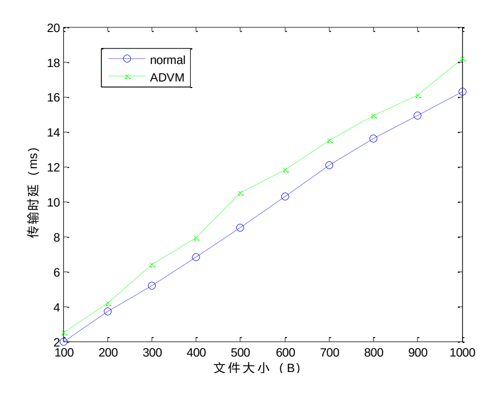


图 6　Alice 为固定节点时的开销

由图 6 可知，与正常通信相比，传输同样大小的文件，ADVM 方案的开销并未显著增加，且传输过程中未出现数据包乱序问题，Alice 能完整恢复出所传输的文件。

针对第二种场景，令 Alice 发生真实移动至子网 2001:da8:2023::/48，并按照场景一中的方法对 ADVM 方案的开销进行测试，其测试结果如图 7 所示。

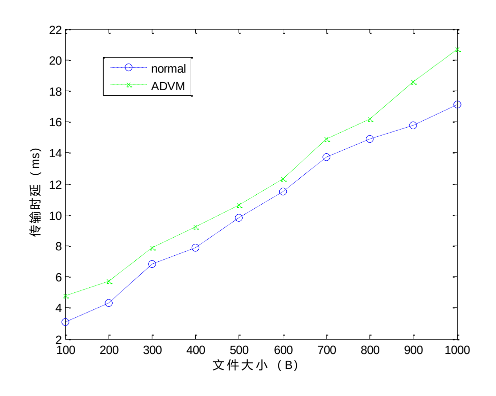


图 7　Alice 为移动节点时的开销

由图 7 可知，当 Alice 发生真实移动时，ADVM 方案的开销相比第一种场景有所增加，这是因为 Alice 执行了移动 IPv6 过程，但与正常通信相比，其开销并未显著增加。

由上可知，测试结果与 3.2 节的分析结论一致，说明了 ADVM 方案的额外开销并未影响节点间的正常通信。

3.2　ADVM 抗流量分析能力测试

为验证 ADVM 的抗攻击能力，假设攻击者 Attacker 具备截获 Bob1 和 Bob2 发出的数据包的能力，攻击者分别对 ADVM 启用前后，Bob1 和 Bob2 在 5 min 通信时间内的数据包的地址分布情况的统计分析结果如图 8 所示。

由图 8 可知，ADVM 启用之前，攻击者 Attacker 从截获到的流量可分析出 Alice 与 Bob1 和 Bob2 之间保持密切通信的关系；ADVM 启用之后，攻击者 Attacker 从截获到的流量中分析出的是 Bob1 和 Bob2 与 A_1 和 A_2 之间的通信关系较为密切，而与 Alice 之间的通信关系并不密切，提高了攻击难度。

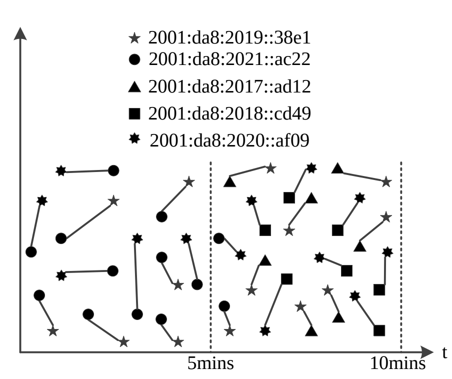


图 8　ADVM 启用前后流量分析图

3.3　抗 DoS 攻击能力测试

假设攻击者经过流量分析发现，A_1 和 A_2 是与 Bob1 和 Bob2 通信的关键节点，若能对其实施 DoS 攻击，那么 Alice 与 Bob1 和 Bob2 之间的通信必然受到攻击，然而在实际网络中，A_1 和 A_2 是的数量和节点都是随机变化的，为进一步测试 ADVM 的抗 DoS 攻击能力，在实验网络中逐步增加虚拟移动代理的部署，并进行相应测试，其测试结果如图 9 所示。

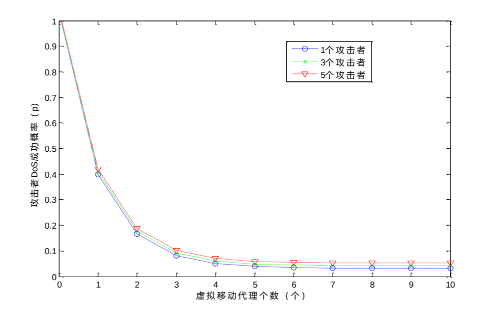


图 9　不同个数攻击者 DoS 攻击成功率与 VMA 之间的关系

由图 9 可知，随着网络中虚拟移动代理个数的增加，攻击者成功实施 DoS 攻击的概率越低，但是攻击者个数的增加并没有显著增加 DoS 攻击成功率，与 3.1 节的分析结果一致。

3.4　对比测试

文献[16]中提出一种基于伴动的移动 IPv6 位置隐私保护方案 FBLPC，通过位于与移动节点不同链路的节点配合，形成 MN 移动至外地的“伴动”情形。虽然该方案可以保护移动节点的位置，但是其安全性取决于 FRN，存在单点失效问题。

接下来，本文将从系统性能和方案安全性两个方面对这 ADVM 方案和 FBLPC 方案进行对比测试。首先，在传输相同大小文件（分别为 1 MB、2 MB、3 MB、4 MB）时系统开销测试结果如图 10 所示。

由图 10 可知，传输相同大小的文件时，ADVM 的开销略比 FBLPC 大，但仍然处于毫秒级。

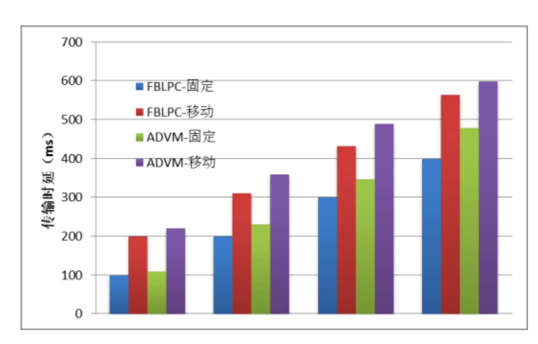


图 10　ADVM 与 FBLPC 方案开销对比

然后，分别在实验网络中部署 1、3、5 个攻击者，攻击者发起 10 次 DoS 攻击，对两种方案的抗 DoS 攻击能力进行了对比测试，其测试结果如图 11 所示。

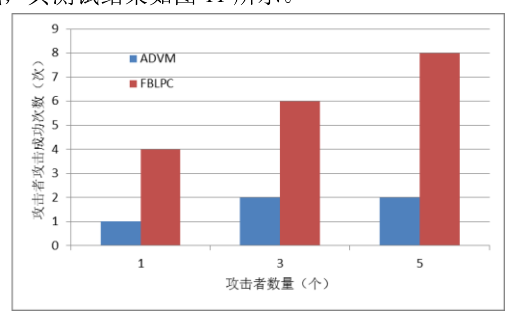


图 11　ADVM 与 FBLPC 抗 DoS 攻击能力对比

由图 11 可知，ADVM 比 FBLPC 方案的抗 DoS 攻击能力更强，综合来看，ADVM 方案以较小的额外开销，换来了更好的网络防护能力。

4　结束语

利用 IPv6 对移动特性的良好支持与多转交地址注册机制，

本文提出一种基于虚拟移动的 IPv6 主动防御方案，通过为受保护 IPv6 节点随机分配多个动态变化的转交地址，使攻击者无法准确辨识目标节点是否发生真实移动及其位置，从而无法对其实施 DoS 攻击等。与已有方案相比，ADVM 方案既能保证主动防御过程中的通信持续不间断，又能以较小的系统开销换取防护能力的较大提升。与移动 IPv6 相比，移动 IPv4 的主要不同之处在于：a)移动节点可以直接向通信对端发送数据，而通信对端必须经过家乡代理向移动节点发送数据；b)移动 IPv4 中没有返回路由可达过程；c)IPv4 中需要使用 IP-in-IP 隧道进行数据传输。由于 IPv6 与 IPv4 将长期共存，虽然移动 IPv4 有别于移动 IPv6 的不同之处会增加系统开销，部分模块功能无法应用于移动 IPv4 中，但是虚拟移动思想仍然适用于 IPv4 网络环境。因此，本文下一步的主要工作是将该方案的各个功能模块进行细化，使虚拟移动方案在 IPv6/IPv4 共存环境中能够选择最优的虚拟移动策略，从而以较小的系统开销实现对共存环境下目标节点的有效防护。

参考文献：

[1] https://www. iab. org/2016/11/07/iab-statement-on-ipv6/ [EB/OL]. [2016-11-07].

[2] http://politics. people. com. cn/n1/2017/1127/c1001-29668295. html [EB/OL]. [2017-11-27].

[3] http://tech. sina. com. cn/i/2012-02-16/08086731105. shtml [EB/OL]. [2012-02-16].

[4] 蔡桂林，王宝生，王天佐，等. 移动目标防御技术研究进展 [J]. 计算机研究与发展, 2016, 53 (5): 968-987.

[5] Kewley D, Fink R, Lowry J, *et al.* Dynamic approaches to thwart adversary intelligence gathering [C]// Proc of IEEE DARPA Information Survivability Conference & Exposition II. Piscataway, NJ: IEEE Press, 2001: 176-185.

[6] Antonatos S, Akritidis P, Markatos E P, *et al.* Defending against hitlist worms using network address space randomization [J]. Computer Networks, 2007, 51 (12): 3471-3490.

[7] Lee H C J, Thing V L L. Port hopping for resilient networks [C]// Proc of the 60th Vehicular Technology Conference. Piscataway, NJ: IEEE Press, 2004: 3291-3295.

[8] Badishi G, HerzbergA A, Keidar I. Keeping denial-of-service attackers in the dark [C]// Proc of Distributed Computing. Berlin: Springer, 2005: 18-32.

[9] 石乐义，贾春福，吕述望. 基于端信息跳变的主动网络防护研究 [J]. 通信学报, 2008, 29 (2): 106-110

[10] Jafarian J H, Al-Shaer E, Duan Qi. OpenFlow random host mutation: Transparent moving target defense using software defined networking [C]// Proc of the 1st Workshop on Hot Topics in Software Defined Networks. New York: ACM Press, 2012: 127-132.

[11] Al-shaer E, Duan Qi, Jafarian J H. Random host mutation for moving target defense [C]// Proc of Security and Privacy in Communication Networks. Berlin: Springer, 2013: 310-327.

[12] Jafarian J H H, Al-Shaer E, Duan Qi. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers [C]// Proc of the 1st ACM Workshop on Moving Target Defense. New York: ACM Press, 2014: 69-78.

[13] Dunlop M, Groat S, Urbanski W, *et al.* MT6D: a moving target IPv6 defense [C]// Proc of MILCOM 2011. Piscataway, NJ: IEEE Press, 2011: 1321-1326.

[14] 刘慧生，王振兴，郭毅. 一种基于多穴跳变的 IPv6 主动防御模型 [J]. 电子与信息学报, 2012, 34 (7): 1715-1720

[15] RFC 5648, Multiple care-of addresses registration [S].

[16] 刘慧生，王振兴，张连成. 基于佯动的移动 IPv6 位置隐私保护方案 [J]. 计算机研究与发展, 2012, 49 (Suppl.): 74-81.